UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/691,170	10/22/2003	Brant L. Candelore	80398P558D	6531

8791 7590 04/17/2008

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
LASHLEY, LAUREL L	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
04/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/691,170	CANDELORE, BRANT L.	
	Examiner	Art Unit	
	LAUREL LASHLEY	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 December 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,23-25,27 and 32-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,23-25,27 and 32-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/27/2007 has been entered.

2. Claims 1-8, 23-25, 27 and 32-35 are pending and have been examined.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 12/27/2007 was filed before the mailing date of any final Office Action. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1 – 2 and 4 - 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al. in US Patent No. 6157719 (hereinafter Wasilewski) and further in view of Akiyama et al. in US Patent No. 5784464 (hereinafter Akiyama).

5. With regard to claim 1, and similar claims 23 and 32 Wasilewski discloses a descrambler integrated circuit (IC) adapted to receive scrambled digital content, a message and an encrypted descrambling key (Fig. 2B), comprising:

a local memory to store a unique key (Fig. 2B: items 232 and Kpr);

a first process block to decrypt a message using the unique key to produce a key, (Fig. 2B, Items: 234, E_{kpr}(MSK), Kpr, and MSK indicate process block to decrypt a message using unique key to produce a key), the key being formed from a mating key generator being a message (see column 6, lines 39-64, MSK derived of message content being combined with a secret, this secret is all or part of the MSK)

a second process block using the key to decrypt the encrypted descrambling key and to recover a descrambling key; (Fig. 2B: item 236, MSK, E_{msk}(CW), CW indicate second process block using the key to decrypt the encrypted descrambling key and to recover the descrambling key) and

a descrambler using the descrambling key to descramble the scrambled digital content and to produce digital content in a clear format (Fig. 2B: item 238, CW, E_{cw}(service), Service indicate a descrambler using the descrambling key to descrambler the scrambled digital content to produce digital content in a clear format), *but Wasilewski does not disclose* the mating key generator being a message that comprises an identifier manufacturer of a digital device including the descrambler IC and an identifier of a supplier of the scrambled digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider.

On the other hand, Akiyama discloses a message comprises an identifier of a supplier of the scrambled digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider (column 14, lines 35-65).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention to modify the method of Wasilewski to include an identifier manufacturer of a digital device including the descrambler IC and an identifier of a supplier of the scrambled

digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider, as taught by Akiyama to utilize supplier identification in the key generation process to provide further protection of the digital content (column 14, lines 35-65).

With regard to claim 2, Wasilewski discloses the descrambler IC (Fig. 2B), wherein the unique key is loaded into the local memory during manufacture of the descrambler IC (column 11: lines 57-63).

With regard to claim 4, Wasilewski discloses the descrambler IC (Fig. 2B), wherein the key is formed by encrypting the mating key generator using the unique key. (Fig. 2B, items: 234, Ekp,(MSK), Kpr, and MSK indicate process block to decrypt a message using unique key to produce a key)

With regard to claim 5, Wasilewski discloses the descrambler IC (Fig. 2B), with the mating key generator (Fig. 2B: item "E_{kpr}(MSK)", "E_{msk}(CW)", and "E_{cw}(Service)", indicate mating key generator(s)) that enables transmission of the scrambled digital content and the mating key generator message to the descrambler IC (Fig. 3: Item 331, "Transmission Medium", Item 329 "encrypted content", Item 315 "EMM", and Item 333, "Service Reception".

However Wasilewski does not disclose the descrambler, wherein the mating key generator further comprises an identifier that identifies a provider of a system that enables transmission of the scrambled digital content and the mating key generator message to the descrambler IC.

On the other hand, Akiyama discloses a message further comprises an identifier that identifies a provider of a system that enables transmission of the scrambled digital content and the mating key generator message to the descrambler IC (see column 14, lines 35-65).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Wasilewski to include an identifier of a supplier of the scrambled digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider, as taught by Akiyama to utilize supplier identification in the key generation process to provide further protection of the digital content (column 14, lines 35-65).

Claims 6-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski and Akiyama further in view of Ferraro in US Patent No. 5151782.

With regard to claim 6, Wasilewski discloses the descrambler IC (Fig. 2B), with the mating key generator (Fig. 2B: item "E_{kpr}(MSK)", "E_{msk}(CW)", and "E_{cw}(Service)", indicate mating key generator(s)), and a conditional access (CA) system which the scrambled digital content is transmitted (Fig. 1: item 101) and a mating key sequence number (col. 6: lines 32-37).

However, Wasilewski does not disclose the mating key generator further comprises (i) an identifier that identifies a conditional access (CA) system provider over which the scrambled digital content is transmitted

On the other hand, Ferraro discloses the mating key generator further comprises (i) an identifier that identifies a conditional access (CA) system provider over which the scrambled digital content is transmitted (col. 5: lines 33-35, "Video Cipher II" indicates an identifier that identifies a conditional access (CA) system provider over which the scrambled digital content is transmitted).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Wasilewski to include (i) an identifier that identifies a conditional access (CA) system provider over which the scrambled digital

content is transmitted, as taught by Ferraro to utilize supplier identification in the key generation process to provide further protection of the digital content (col. 3: lines 4-6).

With regard to claim 7 Wasilewski discloses the descrambler IC (Fig. 2B) wherein the first process block and the second process block are logic operating in accordance with one of the following: Data Encryption Standard (DES, Advanced Encryption Standard (AES), and Triple DES (Fig. 3: item 339 and 343).

Claim 8 is rejected under 35 USC 103(a) as unpatentable over Wasilewski and Akiyama further in view of Alve et al in US Pat. No. 6959090 (hereinafter Alve).

With regard to claim 8 and similar claim 33, Wasilewski disclose the descrambler IC (Fig. 2B) with the unique key (Fig. 2B: items 232 and Kpr). However, Wasilewski does not disclose the unique key is a one-time programmable value that cannot be read or overwritten once programmed.

Alve, on the other hand, discloses a one-time programmable value that cannot be read or overwritten once programmed (Fig. 4: item 203 and 204).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Wasilewski to include such that the unique key is a one-time programmable value that cannot be read or overwritten once programmed, as taught by Alve to protect recorded content from illicit reproduction and distribution (col. 1, lines 27-28).

Claims 23 – 25, 27 and 35 are rejected under 35 USC 103(a) as unpatentable over Wasilewski and Akiyama in view of Alve, and further in view of Kocher et al. in US Pat. No. 6640305 (hereinafter Kocher).

With regard to claim 23, Wasilewski discloses a descrambler integrated circuit adapted to receive scrambled digital content and to descramble the scrambled digital content (Fig. 2B), comprising:

a first process block to decrypt a message using a unique key to produce a first key (Fig. 2B, Items: 234, E_{kpr}(MSK), Kpr, and MSK indicate process block to decrypt a message using unique key to produce a key), the message includes a mating key generator being a message (see column 6, lines 39-64, MSK derived of message content being combined with a secret, this secret is all or part of the MSK) ;

a second process block to receive an encrypted second key and, using the first key, to decrypt the encrypted second key in order to recover the second key in a non-encrypted format, the encrypted second key (Fig. 2B: item 236, MSK, E_{msk}(CW), CW indicate second process block using the key to decrypt the encrypted descrambling key and to recover the descrambling key in a non-encrypted format); and

a descrambler using the second key in the non-encrypted format to descramble the scrambled digital content and to produce digital content in a clear format (Fig. 2B: item 238, CW, E_{cw}(service), CW and Service indicate a descrambler using the descrambling key in the non-encrypted format to descrambler the scrambled digital content to produce digital content in a clear format).

However, Wasilewski does not disclose the unique key is a one-time programmable value that cannot be read or overwritten once programmed.

Alve, on the other hand, discloses a one-time programmable value that cannot be read or overwritten once programmed (Fig. 4: item 203 and 204) *but does not expressly disclose* the mating key generator that comprises an identifier of one or more of (i) a manufacturer of a digital

device employed with the descrambler IC, (ii) a service provider identifier, and (iii) a conditional access (CA) provider identifier.

However Akiyama discloses the mating key generator that comprises an identifier of one or more of (i) a manufacturer of a digital device employed with the descrambler IC, (ii) a service provider identifier, and (iii) a conditional access (CA) provider identifier (col. 14: lines 35-65).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Wasilewski to include such that the unique key is a one-time programmable value that cannot be read or overwritten once programmed, as taught by Alve to protect recorded content from illicit reproduction and distribution (col. 1, lines 27-28) and to incorporate disclose the mating key generator that comprises an identifier of one or more of (i) a manufacturer of a digital device employed with the descrambler IC, (ii) a service provider identifier, and (iii) a conditional access (CA) provider identifier as taught by Akiyama to utilize supplier identification in the key generation process to provide further protection of the digital content (col. 14: lines 35-65).

Furthermore, neither Wasilewski nor Alve discloses a first process block to encrypt a message using a unique, one-time programmable key to produce a first key;

Kocher, on the other hand discloses a first process block (Fig. 11: item 1130) to encrypt (Fig. 11: Item "Pseudo-asymmetric transform" and 1140) a message using a unique one-time programmable key to produce a first key.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify methods of Wasilewski and Alve to include such that the first process block to encrypt a message using a unique, one-time programmable key to produce a first key, as taught by Kocher to distribute content decryption keys in encrypted form to a tamper-resistant cryptographic unit to prevent any attacks (col. 2: lines 45-51).

With regard to claim 24, Wasilewski discloses the descrambler IC (Fig. 2B), wherein the encrypted second key is an encrypted service key (Fig. 2B: item "E_{msk}(CW)" indicates encrypted service key) associated with at least one selected tier of service (Fig. 22: item 2229, col. 36: lines 56-57, IPPV or NVOD indicates tier of service).

With regard to claim 25, Wasilewski discloses the descrambler IC (Fig. 2B) with the encrypted second key is an encrypted descrambling key (Fig. 2B: item "E_{msk}(CW)" indicates encrypted service key is an encrypted descrambling key).

However, neither Wasilewski nor Alve discloses the encrypted second key is an encrypted descrambling key from a smart card in communication with the descrambler IC.

Kocher, on the other hand, discloses the encrypted second key is an encrypted descrambling key from a smart card in communication with the descrambler IC (col. 21: lines 47-49).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify methods of Wasilewski and Alve to include such that the encrypted second key is an encrypted descrambling key from a smart card in communication with the descrambler IC, as taught by Kocher to distribute content decryption keys in encrypted form to a tamper-resistant cryptographic unit to prevent any attacks (col. 2: lines 45-51).

With regard to claim 27, Wasilewski discloses the descrambler IC (Fig. 2B) wherein the mating key generator (Fig. 2B: Item MSK indicates a mating key generator) encrypted by the first process block further using the unique key to produce a result being the first key (Fig. 2B, Items: 234, E_{kpr}(MSK), Kpr, and MSK indicate process block to decrypt a message using unique key to produce a key)

With regard to claim 35, Wasilewski discloses the descrambler IC (Fig. 2b) wherein the encrypted second key is the second key encrypted to a mating key being a value retrieved from a remote server using the mating key generator and a serial number of a digital device implemented with the descrambler IC (Fig. 2B: item 236, MSK, $E_{msk}(CW)$).

Claims 3, 32 and 34 is rejected under 35 USC 103(a) as unpatentable over Wasilewski and Akiyama in view of Zhang et al (US Pat. No. 6550008), hereafter "Zhang".

With regard to claim 3, Wasilewski discloses the descrambler IC (Fig. 2B) with the second process block (Fig. 2B: Item 236). However, Wasilewski does not disclose the descrambler IC, wherein the second process block is a finite state machine.

However, Zhang discloses the descrambler IC, wherein the second process block is a finite state machine (col. 5: lines 55-60).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Wasilewski to include the second process block is a finite state machine, as taught by Zhang to improve protection scheme for broadcast signals or other transmitted information (col. 1: lines 40-43).

With regard to claim 32, Wasilewski discloses a descrambler integrated circuit adapted to receive scrambled digital content and to descramble the scrambled digital content (Fig. 2B), comprising:

a first process block to decrypt a message using a unique key to produce a first key (Fig. 2B, Items: 234, $E_{kpr}(MSK)$, Kpr, and MSK indicate process block to decrypt a message using unique key to produce a key), the message includes a mating key generator being a message (see column 6, lines 39-64, MSK derived of message content being combined with a secret, this secret is all or part of the MSK) ;

a second process block to receive an encrypted second key and, using the first key, to decrypt the encrypted second key in order to recover the second key in a non-encrypted format, the encrypted second key (Fig. 2B: item 236, MSK, E_{msk}(CW), CW indicate second process block using the key to decrypt the encrypted descrambling key and to recover the descrambling key in a non-encrypted format); and

a descrambler using the second key in the non-encrypted format to descramble the scrambled digital content and to produce digital content in a clear format (Fig. 2B: item 238, CW, E_{cw}(service), CW and Service indicate a descrambler using the descrambling key in the non-encrypted format to descrambler the scrambled digital content to produce digital content in a clear format).

However, Wasilewski does not discloses a first process block controlled by a non-CPU based state machine to decrypt a message using the unique key to produce a key; a second process block controlled by a non-CPU based state machine using the key to decrypt the encrypted descrambling key and to recover a descrambling key.

However, Zhang discloses a first process block controlled by a non-CPU based state machine (col. 5: lines 57-59) to decrypt a message using the unique key to produce a key; a second process block controlled by a non-CPU based state machine (col. 5: lines 57-59) using the key to decrypt the encrypted descrambling key and to recover a descrambling key *but does not expressly disclose* the message is a mating key generator that comprises an identifier of one or more of (i) a manufacturer of a digital device employed with the descrambler IC, (ii) a service provider identifier, and (iii) a conditional access (CA) provider identifier.

However Akiyama discloses the message is a mating key generator that comprises an identifier of one or more of (i) a manufacturer of a digital device employed with the descrambler

IC, (ii) a service provider identifier, and (iii) a conditional access (CA) provider identifier (col. 14: Lines 35-65).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Wasilewski to include a first process block controlled by a non-CPU based state machine to decrypt a message using the unique key to produce a key, and a second process block controlled by a non-CPU based state machine (col. 5: lines 57-59) using the key to decrypt the encrypted descrambling key and to recover a descrambling key, as taught by Zhang to improve protection scheme for broadcast signals or other transmitted information (col. 1: lines 40-43) and to incorporate that the message is a mating key generator that comprises an identifier of one or more of (i) a manufacturer of a digital device employed with the descrambler IC, (ii) a service provider identifier, and (iii) a conditional access (CA) provider identifier as taught by Akiyama to utilize supplier identification in the key generation process to provide further protection of the digital content (col. 14: lines 35-65).

With regard to claim 34, Wasilewski discloses the descrambler IC (Fig. 2B) wherein the first process block and the second process block are logic operating in accordance with one of the following: Data Encryption Standard (DES, Advanced Encryption Standard (AES), and Triple DES (Fig. 3: item 339 and 343).

Claim 33 is rejected under 35 USC 103(a) as unpatentable over Wasilewski, Akiyama, Zhang and further in view of Alve et al in US Pat. No. 6959090 (hereinafter Alve).

With regard to claim 33, Wasilewski disclose the descrambler IC (Fig. 2B) with the unique key (Fig. 2B: items 232 and Kpr) loaded into memory during manufacture of the descrambler IC (see column 11, lines 55-60). However, Wasilewski does not disclose the

unique key is a one-time programmable value that cannot be read or overwritten once programmed.

Alve, on the other hand, discloses a one-time programmable value that cannot be read or overwritten once programmed (Fig. 4: item 203 and 204).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Wasilewski to include such that the unique key is a one-time programmable value that cannot be read or overwritten once programmed, as taught by Alve to protect recorded content from illicit reproduction and distribution (col. 1, lines 27-28).

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to LAUREL LASHLEY whose telephone number is (571)272-0693. The examiner can normally be reached on Monday - Thursday, alt Fridays btw 7:30 am & 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, Jr. can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Laurel Lashley
Examiner
Art Unit 2132

/L. L./
11 April 2008

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132